значительно затрудняет установление предмета разговора. При прослушивании записи можно сделать о самом факте наличия речи, но нельзя установить смысл слов и тематики разговора.

Рис. 2. Шкала артикуляционной таблицы

Было экспериментально установлено, что «речеподобная» помеха, сформированная путем микширования звуковых дорожек с переменным увеличением уровня громкости, обладает наилучшим эффектом для предотвращения разборчивости речи по сравнению с другими помехами. Для достижения одинаковой словесной разборчивости уровень громкости генератора белого шума должен быть на 9 дБ больше чем у «речеподобной» помехой. Использование данной разновидности помехи обеспечивает на 25 % снижение разборчивости по сравнению с белым шумом.

Список литературы

1. *Фучко М. М.*, *Широких А. В.*, *Захаров А. А.*, *Несговоров Е. С.*, *Оленников Е. А.* Аудиовыход как скрытый канал утечки данных: технологии создания и методы защиты // Вестн. УрФО. Безопасность в информационной сфере. 2016. № 3(21).

УДК 661.3.066

А. В. Шабров, Е. А. Бусыгин
Научный руководитель: аспирант К. Л. Стойчин
Уральский федеральный университет, Екатеринбург

ПРОБЛЕМА ПРИМЕНЕНИЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ ПО КАНАЛАМ СВЯЗИ

Аннотация. В данной статье рассмотрены актуальные вопросы безопасного применения средств криптографической защиты информации при передаче по каналам и линиям связи.

Ключевые слова: средтсва криптографчиеской защиты информации; канал; линия связи; система защиты; аппаратные средства; нарушитель; модель угроз.

В настоящее время средства криптозащиты являются неотъемлемой частью как малого бизнеса, так и предприятий государственного сектора. Если раньше для нанесения финансового вреда компании злоумышленникам чаще всего приходилось проникать на ее территорию, вскрывать помещения и сейфы, то теперь достаточно похитить токен с криптографическим ключом и сделать перевод через систему «клиент — банк», что ведет за собой как потерю репутации для малого и среднего бизнеса, так и ущерб государству. Сегодня к средствам криптографической защиты информации (СКЗИ) относят средства шифрования, средства имитозащиты, средства электронной цифровой подписи, средства кодирования, средства изготовления ключевых документов и сами ключевые документы.

Любая система защиты информации — это комплекс организационно-технических мероприятий, который включает в себя совокупность правовых норм, организационных мер и программно-технических средств защиты, направленных на противодействие угрозам объекту информатизации с целью сведения до минимума возможного ущерба пользователям и владельцам системы. Без организационных мер, наличия четкой организационно-распорядительной системы на объекте информатизации эффективность любых технических СЗИ снижается.

Актуальность проблемы, рассмотренной в данной статье, заключается в том, что в случае применения аппаратных средств СКЗИ возникают незащищенные участки, являющиеся потенциально опасными с точки зрения инцидента информационной безопасности, становясь опасным каналом, через который может произойти утечка информации. В случае, если злоумышленник получает доступ к участку, где циркулирует еще не защищенная информация, то в этом случае применение данного СКЗИ становится бессмысленным, вследствие чего наносится ущерб предприятию.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Например, весьма опасной угрозой являются выставки, на которые многие организации отправляют оборудование из производственной сети со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде.

Перехват данных — серьезная угроза, и, если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно.

На данном этапе исследования целесообразно рассмотреть участок сети, циркулирует еще не защищенная СКЗИ информация. Например: через кори-

дор офисного здания проходит линия связи, в которой информация еще не защищена СКЗИ. Подразделение информационной безопасности утверждает, что если она находится в контролируемой зоне, то угроз для информации, циркулирующей на данном участке и содержащей сведения, составляющие коммерческую тайну, нет. Данное утверждение является ошибочным. Если по данной линии передается конфиденциальная информация, то ее нужно обязательно защищать. В результате получаем, что информация, проходящая по каналу в пределах контролируемой зоны, не является защищенной и существует опасность утечки передаваемой информации.

Чтобы защитить линию, по которой передаются незащищенная информация, необходимо (до внедрения и использования СКЗИ) определить перечень актуальных угроз (модель угроз), определить, для нейтрализации каких из них требуются СЗКИ, определить возможности нарушителей (модель нарушителя).

В самом простом случае идут по пути реализации в одном документе (как правило, модель угроз) и требований ФСТЭК к определению угроз и требований ФСБ к определению угроз и нарушителей. Рассмотрим такой вариант.

При оценке рисков ИБ наиболее опасными считаются угрозы от источников — внутренних пользователей ИС/сотрудников организации, так что, скорее всего, для ИС в целом будут актуальны внутренние нарушители (условно назовем Н3).

При таких актуальных типах нарушителей нам требуется использовать СКЗИ, сертифицированные по классу не ниже КС3.

Разработав модель угроз и выбрав класс, но это еще не означает, что наш канал защищен на 100 %. Чтобы обеспечить достойный уровень защиты линии связи, по которому циркулирует информация, нужно проделать следующие немаловажные процедуры:

1. Издать инструкцию, в которой будут описаны правила пользования СКЗИ, а также будет прописана ответственность за нарушение правил обеспечения безопасности.

2. Оснастить помещения, в которых располагаются СКЗИ, входные двери с обеспечением постоянного закрытия дверей на замок и их открытия только в случае санкционированного прохода.

3. Утвердить правила доступа в помещения, в котором располагаются СКЗИ, в рабочее время, а также в иных нештатных ситуациях.

4. Утвердить список лиц, которые имеют права доступа в помещение, где располагаются СКЗИ.

5. Организовать разграничение контроля доступа к защищаемой информации.

На АРМ и серверах, где установлены СКЗИ необходимо соблюдать следующие правила:

1. Использовать только сертифицированные средства защиты информации от несанкционированного доступа.

2. Использовать сертифицированные средства антивирусной защиты.

УДК 004.056.53

Т. В. Быкова
Научный руководитель: канд. тех. наук У. В. Михайлова
Магнитогорский государственный технический университет,
Магнитогорск

ОЦЕНКА ЗАЩИЩЕННОСТИ РАДИОКАНАЛА

Аннотация. В данной статье рассмотрены актуальные проблемы обнаружения утечки информации по радиоканалам связи.

Ключевые слова: информация; безопасность; инженерно-техническая защита информации; защита информации; радиомониторинг; закладное устройство; специальное техническое средство.

В настоящее время существует огромное разнообразие современных специальных технических средств (СТС), использующихся для несанкционированного доступа к информации (радиозакладки). Радиозакладки используют сложные типы сигналов, затрудняющие их обнаружение, а передача перехваченной информации производится по легальным каналам связи.

Актуальным вопросом в задачах поискового радиоконтроля считается анализ не только широковещательных пакетов, но и пакетов мобильных устройств, получение из которых в разрешенных рамках максимума полезной информации позволяет идентифицировать каждое такое устройство и локализовать его местоположение. В настоящее время, как показывает практика, радиомониторинг должен быть круглосуточным, так как это единственный способ проследить за тем, как ведет себя сигнал и как он соотносится с различными важными событиями на охраняемом объекте. Также это позволяет обнаруживать закономерности во времени появления в эфире и сравнить текущие спектры сигналов с ранее полученными.

Не зная алгоритма входа радиозакладки в эфир, крайне сложно обнаружить ее сигнал. Поэтому очень важно следить за отображением спектра сигналов в виде «водопада», позволяющего наблюдать за изменениями радиочастотного спектра с привязкой во времени. Появляется возможность вести базу данных непрерывно и круглосуточно, не теряя ни одного сигнала. Иногда закладное